অ্যাডভান্সড পারসিস্ট্যান্ট থ্রেট সাধারণ বিশ্লেষণ

দেবাশীষ পাল
ইনফরমেশন সিকিউরিটি স্পেশালিস্ট, বিজিডি ই-গভ সার্ট

অ্যাডভান্সড পারসিস্ট্যান্ট থ্রেট (এপিটি) এক ধরনের সাইবার আক্রমণ, যা দিয়ে সাইবার আক্রমণকারীরা বা নেটওয়ার্কে অবৈধ অনুপ্রবেশকারী বা অবৈধ অনুপ্রবেশকারীদের দল কমপিউটার ব্যবহারকারী বা সিস্টেম অ্যাডমিনদের অজান্তে কমপিউটার নেটওয়ার্কে দীর্ঘ সময় উপস্থিত থেকে ও ক্রমাগত কমপিউটার হ্যাকিং প্রসেস দিয়ে টার্গেট নেটওয়ার্কে খুব সংবেদনশীল তথ্য (highly sensitive data) বা মেধা সম্পত্তি (Intellectual property) চুরি করা, critical Critical অবকাঠামোগুলোর ব্যাপক ক্ষতিসাধন (যেমন– ডাটাবেজ মুছে ফেলা বা তথ্য পরিবর্তন করা) বা টার্গেট নেটওয়ার্কের পূর্ণ দখল নিতে পারে। এপিটি সাইবার আক্রমণ বেশ জটিল ও বিভিন্ন ধাপে করা হয়।

এই লেখায় আমরা এপিটি এর সাধারণ বিশ্লেষণ আলোচনা করব। সাইবার সচেতনতা বাড়ানোর লক্ষ্যে এ লেখাটি তৈরি করা হয়েছে। এপিটি ধরনের সাইবার আক্রমণের প্রথম ধাপে সাইবার আক্রমণকারীরা সিস্টেমে দুর্বলতা খুঁজে বের করে সেই সিস্টেমের পূর্ণ দখল নিয়ে "advanced Advanced" ম্যালওয়্যার ব্যবহার করে। নির্দিষ্ট টার্গেট থেকে তথ্য নেয়া ও টার্গেটটি পর্যবেক্ষণ করার জন্য টার্গেট নেটওয়ার্কের বাইরে কোনো command Command and control Control system System সাথে যোগাযোগ যাতে "persistentPersistent" থাকে সেটি নিশ্চিত করে এবং সম্পূর্ণ প্রক্রিয়ার পেছনে মানব সম্পৃক্ততা রয়েছে, যা কমপিউটার ব্যবহারকারী বা সংস্থাসমূহের কাছে হুমকি (Tthreat) হিসেবে বিবেচিত হয়, তাই এই সম্পূর্ণ সাইবার আক্রমণকে Advanced Persistent Threat (APT) বলা হয়।

সংক্ষেপে এপিটি একটি নেটওয়ার্ক আক্রমণ, যা অবৈধ অনুপ্রবেশকারী নেটওয়ার্কে দীর্ঘ সময় উপস্থিত থেকে গোপনে ব্যাকডোর (backdoor) স্থাপন করে বিভিন্ন তথ্য সংগ্রহ করে নেটওয়ার্ক থেকে বের হয়ে যায়।

জিরোডে এবং সাইবার হামলা

অনেক এপিটি আক্রমনে জিরো ডে দুর্বলতা ব্যবহার করা হয়েছে। জিরো ডে দুর্বলতা হলো সফটওয়্যারে নিরাপত্তা দুর্বলতা, যা সফটওয়্যার ভেন্ডরদের অজানা থাকে। অনেক ক্ষেত্রে হ্যাকার বা হ্যাকারদল জিরো ডে দুর্বলতা বের করে থাকে এবং সফটওয়্যার ভেন্ডর সচেতন হয়ে উঠবার আগেই সেই নিরাপত্তা দুর্বলতা ব্যবহার করে কমপিউটার ব্যবহারকারীর সিস্টেমের পূর্ণ দখল নিয়ে থাকে। অনেক ক্ষেত্রে সাইবার আক্রমণকারীরা ফিশিং ইমেইলগুলোতে সংযুক্তি হিসেবে প্রেরিত ওয়ার্ড অথবা পিডিএফ ডকুমেন্টে ক্ষতিকারক স্ক্রিপ্ট বা ম্যাক্রো দিয়ে থাকে, যার মাধ্যমে ক্ষতিকারক কোড বা অ্যাপ্লিকেশন, কমপিউটার ব্যবহারকারীর অজান্তে চালু হয়ে যায় এবং কমপিউটারটি সাইবার আক্রমণকারীর নিয়ন্ত্রণে চলে আসে।

এপিটি আক্রমণের সাধারণ ধাপ বিশ্লেষণ

একটি এপিটি আক্রমণের প্রতিটি পদক্ষেপ পরিকল্পিত এবং খুব সাবধানে নেয়া হয়। এর মধ্যে রয়েছে সংগঠনের আইটি অবকাঠামো, malware engineering, social engineering, undetected data extraction-এর মতো পদক্ষেপ।

লক্ষ্য নির্বাচন ও তথ্য সংগ্রহ

এপিটি আক্রমণের প্রথম পর্যায়ে টার্গেট অর্গানাইজেশন (target organization) নির্বাচন করা হয়। এই ধাপের পর্যায়ে সাইবার আক্রমণকারীরা টার্গেট অর্গানাইজেশনের ওয়েবসাইট, তাদের কর্মকর্তাদের resumesResumes/CV বিশ্লেষণ, বিভিন্ন ধরনের ওয়েবে তা বিশ্লেষণ করে আক্রমণকারীরা টার্গেট নেটওয়ার্কে ব্যবহার হয়। তারা এমন সফটওয়্যার, আইটি (সিস্টেম, নেটওয়ার্ক) অবকাঠামো একটি সাধারণ ডিজাইনে বের করার চেষ্টা করে। এ ক্ষেত্রে অপরাধীরা যত বেশি তথ্য সংগ্রহ করবে, তাদের টার্গেট নেটওয়ার্কে অনুপ্রবেশের সম্ভাবনা আরও বেড়ে যায়।

এন্ট্রি পয়েন্ট ও কম্প্রোমাইজড মেশিনে Compromised Machine-এ ম্যালওয়ার স্থাপন

বেশিরভাগ পরিস্থিতিতে আক্রমণকারীরা তাদের টার্গেট কোম্পানির কর্মকর্তাদের লক্ষ্য করে ফিশিং ই-মেইল প্রচারাভিযান ব্যবহার (phishing email campaign) ও সামাজিক প্রকৌশল কৌশল প্রয়োগ (social engineering techniques) করে থাকে এবং কমপিউটার ব্যবহারকারীকে তাদের প্রেরিত ফিশিং ই-মেইলে ডকুমেন্ট ফাইল ওপেন অথবা লিংকে ক্লিক করতে প্ররোচিত করে। এক্ষেত্রে অনেক সময় জিরো ডে দুর্বলতা ব্যবহার করা হয়।

কমপিউটার ব্যবহারকারীর কমপিউটারটি সাইবার আক্রমণকারীর নিয়ন্ত্রণে চলে আসামাত্রই আক্রমণকারীরা কম্প্রোমাইজড মেশিনে ম্যালওয়্যার (যা তাদের কমান্ড এবং কন্ট্রোল যোগাযোগ করতে পারে) ও সাধারণত কাস্টমাইজড Rremote Aadministration Ttool (RAT) স্থাপন করে থাকে, যার মাধ্যমে লক্ষ্যবস্তুর ওপর গোপনে নজরদারি ও তথ্য চুরি করতে থাকে।

Escalate privilegest

বিভিন্ন ধরনের privileges escalation exploit পাসওয়ার্ড ক্র্যাকমেথড ব্যবহার করে কমপিউটারে Administrator privileges, উইন্ডোজ ডোমেইন অ্যাকাউন্টের পাসওয়ার্ড বা সার্ভার অ্যাকাউন্টের পাসওয়ার্ড বের করার চেষ্টা করে। এ সময় আক্রমণকারীরা কী-লগার ব্যবহার করে, ARP স্পুফিং, বিভিন্ন ধরনের হুকিং মেথড, pass the hash, brute force attack ইত্যাদি মেথড ব্যবহার করতে পারে।

Lateral movement

আক্রমণকারীরা অন্যান্য ওয়ার্কস্টেশন, সার্ভার এবং পরিকাঠামো তাদের ওপর তথ্য সংগ্রহ ও সেইসব সিস্টেমের নিয়ন্ত্রণ নেয়ার চেষ্টা করে।

Maintain Presencet

আক্রমণকারীরা যাতে যেকোনো সময় নেটওয়ার্কে অনুপ্রবেশ করতে পারে এবং নেটওয়ার্ক, সিস্টেমের নিয়ন্ত্রণ নিতে পারে তা নিশ্চিত করার জন্য বিভিন্ন ধরনের tools ইনস্টল করে (যেমন command line tools : netcat বা কাস্টম connection tools)।

Complete Mission IData Exfiltrationt

টার্গেট নেটওয়ার্ক থেকে অননুমোদিত তথ্য স্থানান্তর করে (Data Exfiltration) মিশন সম্পূর্ণ করা।

সতর্কতামূলক পদক্ষেপ

সাইবার ডিফেন্স ইন ডেপথ কৌশলের (defense-in-depth strategy) সাহায্যে এই ধরনের সাইবার আক্রমণ প্রতিহত করা যেতে পারে। নেটওয়ার্ক লগ বিশ্লেষণ এবং বিভিন্ন উৎস থেকে লগ correlation করে (এক্ষেত্রে SIEM সহায়তা নেয়া যেতে পারে) APT কার্যক্রম শনাক্ত করা যেতে পারে। নেটওয়ার্ক, সিস্টেম, asset management (ব্যবহৃত

Reference URL
https://en.wikipedia.org/wiki/Advanced_persistent_threat
http://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/